On Power Integral Bases for Certain Abelian Fields

September, 2004

MOTODA Yasuo

On Power Integral Bases for Certain Abelian Fields

A Thesis in

Mathematics

By

MOTODA Yasuo

Doctor of Science

September, 2004

Supervisor : NAKAHARA Toru

Contents

Acknowledgments

First, the author wishes to express his gratitude to **Dr. Syed Inayat Ali Shah** (Doctor Course student in 1998-2001) and **Prof. Toru Nakahara** for their valuable advices.

In 1999, **Prof. Masanori Kôzaki** suggested to him studying Fibonacci sequences and Number Thoery under **Prof. Nakahara**.

In 2001, the author attended at the final phd seminar by **Mr. Shah** in Saga University, and then the author was able to start calculating Hasse's problem[MNS].

Since then, **Prof. Nakahara** recommends him to present several his new results at the international conferences in the Republic of Korea and in Japan, and so the author has been able to meet many researchers of Number Theory.

1. Introduction

Let $\boldsymbol{Z}$ be the ring of rational integers and let Z_F be the ring of integers in an algebraic number field F with extension degree n over the rationals $\boldsymbol{Q}$. One says that Z_F has a power integral basis θ of Z_F when Z_F is generated by an integer θ as $\boldsymbol{Z}$-free module, i.e., $Z_F = \boldsymbol{Z}[1, \theta, \cdots, \theta^{n-1}]$ and in this case F is also called monogenic.

Hasse's problem of characterizing whether Z_F is of monogenesis or not has been treated by Dummit and Kisilevsky [DK], Gaál [Ga_2], Gras [Gr_1, Gr_2], Huard, Spearman and Williams [HSW], Leopoldt [Le], Schertz [Sc], Thérond [Th], Washington [Wa] and others. Gaál, Pethő, Pohst, Győry and Olajos gave algorithms for determining the power bases of the rings of algebraic integers of certain algebraic number fields and provided several monogenic examples [Ga_1, GPP, Gy_2, Ol]. Pethő and Kovác gave connections between power integral bases and radix representations in algebraic number fields [Ko, KP, Pe]. By calculating the discriminant of an integer of Z_F, Nakahara, Shah and Motoda determined whether Z_F is monogenic or not for some cyclotomic fields [M_2, M_3, MN_1, MNS, Nak_1, Nak_2, Nak_3, Nak_4, Nak_5, SN, Sh] and Robertson, Nakahara, Shah and Motoda exhibited the integral power bases for some cyclotomic fields [M_3, MN_1, MN_2, MNS, Ro_1, Ro_2].

Narkiewich [Nar; p. 540] introduces the works of Uchida [Uc] and Győry [Gy_1] in the unsolved problem 6, i.e., *"Find a good necessary and sufficient condition for a field to have index* 1*"*. Moreover concerning the form which gives the value $|d(\xi)|$ in the proof of Theorem 3.1 in Chapter 3, Kubota proposes to study once again a non-essential discriminant (*der außerwesentliche Diskriminantenteiler*) of an algebraic number field in the prospect of the near future of number theory [Ku, p. 228; Ok, Ży].

A survey of researches related to integral power bases is given by Győry [Gy_2].

In Chapter 2, Let K be a biquadratic field over the rationals $\boldsymbol{Q}$, Z_K be the ring of integers of K and k be a quadratic subfield of K. We give following results;
(i) an integral basis of Z_K and the discriminant D_K,

(ii) the relative discriminant $D_{K/k}$,

(iii) the norm residues of K/k for modulo $\mathfrak{p}^r$, where $\mathfrak{p}$ is a prime ideal of k which devides 2 and $\mathfrak{p}^r$ is a $\mathfrak{p}$-component of $D_{K/k}$.

In Chapter 3, Let K be the composite field of imaginary quadratic field $\boldsymbol{Q}(\omega)$ of conductor d and a real abelian field L of conductor f distinct from the rationals $\boldsymbol{Q}$, where, $(d, f) = 1$. In this chapter, we construct new families of infinitely many fields K with the non-monogenic phenomena (1), (2) which supplement [Gr_1, Gr_2] and with monogenic (3).

(1) If $\boldsymbol{Q}(\omega) \neq$ the Gaußfield $\boldsymbol{Q}(i)$, then Z_K is of non-monogenesis.

(2) If $\boldsymbol{Q}(\omega) = \boldsymbol{Q}(i)$, then for a sextic field K, Z_K is of non-monogenesis except for two fields of conductors 28 and 36.

(3) Let $\boldsymbol{Q}(\omega) = \boldsymbol{Q}(i)$. If Z_K has a power basis, then Z_L must have a power basis. Conversely, let L be the maximal real subfield k_f^+ of a cyclic field k_f, namely K be the maximal imaginary subfield of k_{4f} of conductor $4f$. Then Z_K has a power basis.

In Chapter 4, we treat abelian number fields whose Galois groups are 2-elementary. A necessary and sufficient condition for monogenesis of biquadratic fields was given by M.-N. Gras and F. Tanoé [GT, Tan] and a new family of infinitely many monogenic biquadratic fields was constructed by the first author [M_2, M_3]. Assume F to be an abelian field whose Galois group is 2-elementary. If $[F : \boldsymbol{Q}] \geq 16$, then F is non-monogenic, i.e., Z_F has no power integral basis by virtue of the decomposition theory of a prime number (see Lemma 4.1). In the case of $[F : \boldsymbol{Q}] = 8$, by the same lemma, it is enough to investigate the field $F = \boldsymbol{Q}\left(\sqrt{mn}, \sqrt{dn}, \sqrt{\ell}\right)$, where dmn and ℓ are square-free, $d > 0$, $d \equiv 2$, $mn \equiv 3$, $\ell \equiv 1 \pmod 4$. In this chapter, we assume $(dmn,\ \ell) = 1$. Then we will claim that any real 2-elementary abelian field has no power integral basis and our main theorem will state that the complex one has a power integral basis only if $F = \boldsymbol{Q}(\sqrt{-1}, \sqrt{-2}, \sqrt{-3}) = \boldsymbol{Q}(\zeta_{24})$, where, ζ_{24} is the 24-th root of unity.

2. On Biquadratic Fields

2.1. Introduction. Let K be a biquadratic field $\boldsymbol{Q}(\sqrt{dm},\ \sqrt{dn})$, where d, m, n are rational integers with $d > 0$, and dmn is square-free. Let Z_K be the ring of integers of K and let $k = \boldsymbol{Q}(\sqrt{dn})$.

G. Fujisaki[F], M.-N. Gras and F. Tanoé[GT], K. S. Williams[Wi] gave an integral basis of a biquadratic field. Also the author gave it independently. In section 2.2 we calculate it in Theorem 2.1 by using Hasse's conductor-discriminant formula[Wa].

In Theorem 2.2 we give a table of the relative discriminant $D_{K/k}$ by using above formula and the chain theorem.

In sectin 2.3, we determine in Theorm 2.3 the norm residues of K/k for modulo $\mathfrak{p}$-component $\mathfrak{p}^r$ of $D_{K/k}$, where $\mathfrak{p}$ is a prime ideal of k which devides 2.

2.2 An integral basis of K and a table of $D_{K/k}$.

Lemma 2.1 (Hasse's conductor-discriminant formula[Wa]). *Let K be the number field associated to the group X of Dirichlet characters. Then the discriminant of K is given by*

$$d(K) = (-1)^{r_2} \prod_{\chi \in X} f_\chi,$$

where, f_χ denotes the conductor of χ.

Lemma 2.2 (Chain Theorem). *Let k be a subfield of an algebraic number field K and let $D_K, D_k,$ and $D_{K/k}$ be the discriminants of K, k and the relative dicriminant of K over k, respectively. Then we have* ;

$$D_K = {D_k}^{[K:k]} N_k(D_{K/k}),$$

where, the symbol $N_k(\cdot)$ denotes the norm of k over $\boldsymbol{Q}$.

Theorem 2.1 ([F, GT, Wi]). *Let K be a biquadratic field $\boldsymbol{Q}\left(\sqrt{dm}, \sqrt{dn}\right)$, where dmn is square-free. Then an integral basis of Z_K and the discriminant D_K of K are given by the followings;*

(1) *in the case* $dm \equiv dn \equiv 1 \pmod 4$;

$$Z_K = \boldsymbol{Z}\left[1, \frac{1+\sqrt{mn}}{2}, \frac{1+\sqrt{dn}}{2}, \frac{e+\sqrt{mn}+\sqrt{dm}+\sqrt{dn}}{4}\right],$$

$$D_K = d^2m^2n^2, \text{ where } e = \pm 1 \text{ such that } d \equiv m \equiv n \equiv e \pmod 4,$$

(2) *in the cases* $dm \equiv dn \equiv 3 \pmod 4$ *and* (3.1) $dm \equiv dn \equiv 2,\ mn \equiv 1 \pmod 4$;

$$Z_K = \boldsymbol{Z}\left[1, \frac{1+\sqrt{mn}}{2}, \sqrt{dn}, \frac{\sqrt{dm}+\sqrt{dn}}{2}\right],\ D_K = 2^4d^2m^2n^2,$$

(3.2) *in the case* $dm \equiv dn \equiv 2,\ mn \equiv 3 \pmod 4$;

$$Z_K = \boldsymbol{Z}\left[1, \sqrt{mn}, \sqrt{dn}, \frac{\sqrt{dm}+\sqrt{dn}}{2}\right],\ D_K = 2^6d^2m^2n^2.$$

Proof. By Hasse's conductor-discriminant formula, we have $D_K = D_{k_1}D_{k_2}D_{k_3}$, where, $k_1 = \boldsymbol{Q}(\sqrt{mn}),\ k_2 = \boldsymbol{Q}(\sqrt{dn}),\ k_3 = \boldsymbol{Q}(\sqrt{dm})$. First we consider the case (1). Since $D_{k_1} = mn,\ D_{k_2} = dn,\ D_{k_3} = dm$, we have $D_K = mn \cdot dn \cdot dm = d^2m^2n^2$. Let G be the Galois group of K defined by $\left\langle \sigma, \tau; \sqrt{dn}^{\,\sigma} = -\sqrt{dn},\ \sqrt{dm}^{\,\tau} = -\sqrt{dm} \right\rangle$. For $\alpha_i \in Z_K,\ i = 1, 2, 3, 4$, we define $\Delta[\alpha_1, \alpha_2, \alpha_3, \alpha_4]$ by the matrix

$$\begin{vmatrix} \alpha_1 & \alpha_2 & \alpha_3 & \alpha_4 \\ \alpha_1^{\sigma} & \alpha_2^{\sigma} & \alpha_3^{\sigma} & \alpha_4^{\sigma} \\ \alpha_1^{\tau} & \alpha_2^{\tau} & \alpha_3^{\tau} & \alpha_4^{\tau} \\ \alpha_1^{\sigma\tau} & \alpha_2^{\sigma\tau} & \alpha_3^{\sigma\tau} & \alpha_4^{\sigma\tau} \end{vmatrix}.$$

If $\Delta^2[\alpha_1, \alpha_2, \alpha_3, \alpha_4] = \pm D_K$, then we have $Z_K = \boldsymbol{Z}[\alpha_1, \alpha_2, \alpha_3, \alpha_4]$. Now since

$$\frac{1+\sqrt{dm}}{2} \times \frac{1+\sqrt{dn}}{2} = \frac{d-e}{4}\sqrt{mn} - \frac{1-e}{2} \cdot \frac{-1+\sqrt{mn}}{2} + \frac{e+\sqrt{mn}+\sqrt{dm}+\sqrt{dn}}{4},$$

we have $\dfrac{e+1\sqrt{mn}+\sqrt{dm}+\sqrt{dn}}{4} \in Z_K$. Then

$$\Delta^2\left[1, \tfrac{1+\sqrt{mn}}{2}, \tfrac{1+\sqrt{dn}}{2}, \tfrac{e+\sqrt{mn}+\sqrt{dm}+\sqrt{dn}}{4}\right] = 2^{-8}\Delta^2[1, \sqrt{mn}, \sqrt{dm}, \sqrt{dn}]$$

$$= 2^{-8}\begin{vmatrix} 1 & \sqrt{mn} & \sqrt{dm} & \sqrt{dn} \\ 1 & \sqrt{mn}^{\,\sigma} & \sqrt{dm}^{\,\sigma} & \sqrt{dn}^{\,\sigma} \\ 1 & \sqrt{mn}^{\,\tau} & \sqrt{dm}^{\,\tau} & \sqrt{dn}^{\,\tau} \\ 1 & \sqrt{mn}^{\,\sigma\tau} & \sqrt{dm}^{\,\sigma\tau} & \sqrt{dn}^{\,\sigma\tau} \end{vmatrix}^2 = 2^{-8}\begin{vmatrix} 1 & \sqrt{mn} & \sqrt{dm} & \sqrt{dn} \\ 1 & -\sqrt{mn} & \sqrt{dm} & -\sqrt{dn} \\ 1 & -\sqrt{mn} & -\sqrt{dm} & \sqrt{dn} \\ 1 & \sqrt{mn} & -\sqrt{dm} & -\sqrt{dn} \end{vmatrix}^2$$

$$= 2^{-8}d^2m^2n^2 \begin{vmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & -1 & -1 & 1 \\ 1 & 1 & -1 & -1 \end{vmatrix}^2 = d^2m^2n^2.$$

Therefore we have

$$Z_K = \boldsymbol{Z}\left[1, \frac{1+\sqrt{mn}}{2}, \frac{1+\sqrt{dn}}{2}, \frac{e+\sqrt{mn}+\sqrt{dm}+\sqrt{dn}}{4}\right].$$

Similarly, we can obtain the discriminants and integral bases in the cases (2), (3,1) and (3,2). ∎

From conductor-discriminant formula, we see that the relative discriminant $D_{K/k}$ is equal to the conductor $\mathfrak{f}_{K/k}$ of K over k. $D_{K/k}$ is determined by using Theorem 2.1 and chain theorem.

Theorem 2.2. *Let K be a biquadratic field $\boldsymbol{Q}(\sqrt{dn},\ \sqrt{dm})$, where d, m, n are rational integers with $d > 0$,* and *dmn is square-free and put $k = k_1 = \boldsymbol{Q}(\sqrt{dn})$, $k_2 = \boldsymbol{Q}(\sqrt{dm})$. Let $D_{K/k_i},\ i = 1,\ 2$ have the prime power decompositions $\pm 2^{s_i}\prod p \prod q_i,\ i = 1,\ 2$ with $p,\ q$ are odd primes and $\prod p \mid d,\ \prod q_1 \mid n,\ \prod q_2 \mid m$. Then we have the following table of $D_{K/k} = \mathfrak{f}_{K/k}$;*

	0	2	3
0	$\prod q_2$	$\prod q_2$	$\prod q_2$
2	$4\prod q_2$	$\prod q_2$	$2\prod q_2$
3	$8\prod q_2$	$4\prod q_2$	$\prod q_2$ if $\prod q_1 \prod q_2 \equiv 1 \pmod 4$ $2\prod q_2$ if $\prod q_1 \prod q_2 \equiv 3 \pmod 4$

Table of $D_{K/k} = \mathfrak{f}_{K/k}$

Here, the numbers of first raw and first column denote s_1 and s_2, respectively.

Remark 2.1. Halter-Koch([HK], Satz 2) has given a genus field of a ring class-field over k by showing that it can be denoted by a product of biquadratic fields over k and using essentially the above table.

Remark 2.2 ([GT]). A biquadratic field $K = \boldsymbol{Q}\left(\sqrt{dm}, \sqrt{dn}\right)$ is said to be given by the canonical form if the following three conditions are satisfied;

(1) $d,\ m,\ n$ are relatively prime to each other and square-free rational integers,

(2) $dm \equiv dn \pmod 4$, $d > 0$ and $m > n$,

(3) if $dm \equiv dn \equiv 1 \pmod 4$, then $d < n$.

Any biquadratic field K is uniquely presented by the canonical form. In Theorem 2.1, we may assume that K is given by the canonical form. While in Theorem 2.2, we can not use the canonical form, because k is any one of three quadratic subfields of K.

2.3. The norm residues of K/k for modulo $\mathfrak{p}^r$. Let $\mathfrak{p}$ is a prime ideal of k which devides 2. In this section we assume that $\mathfrak{p}$ ramifies in K. In the following theorem we determine the norm residues of K/k for modulo $\mathfrak{p}$-component $\mathfrak{p}^r$ of $D(K/k)$. Here r can be seen by the above table. According to the common use, for simplicity we denote the groups $\{\alpha \in k\ ;\ (\alpha, \mathfrak{p}) = 1\}$ and $\{\nu \in k\ ;\ \nu \equiv N_{K/k}(\Gamma) \pmod{\mathfrak{p}^r}, \Gamma \in K, (\nu, \mathfrak{p}) = 1\}$ by α and ν, respectively[Tak]. ν is said to be the norm residue for modulo $\mathfrak{p}^r$. From the class-field theory, we have $(\alpha : \nu) = 2$[Tak].

Definition. A finite abelian group A is written by a direct product $A_1 \times A_2 \times \cdots \times A_r$ with $e_1 | e_2 | \cdots | e_r$, where, e_j denotes the order of group A_j $(1 \leq j \leq r)$. Then the system $(e_1, e_2, \cdots, e_r)$ is uniquely determined. It is said that the group A has the invariant system $(e_1, e_2, \cdots, e_r)$ or simply that A is of type $(e_1, e_2, \cdots, e_r)$.

Theorem 2.3. *Let k be the quadratic subfield $\boldsymbol{Q}(\sqrt{dn})$ of K and assume a prime ideal $\mathfrak{p}$ of k which dvides 2 ramifies in K/k, we obtain prime residues and norm residues modulo $\mathfrak{p}^r$ as followings, herein K is not given by canonical form and we put*
$c = \dfrac{dn-1}{4}$ *and* $\omega = \dfrac{1+\sqrt{dn}}{2}$;
(1) *if* $dn \equiv 1, dm \equiv 3 \pmod 4$, *then*

$$D(K/k) = 4m,\ 2 = \mathfrak{p},\ r = 2,\ \varphi_k(\mathfrak{p}^2) = 12,$$

(i) *if* $c \equiv 1 \pmod 4$, *then*

$$\alpha = \left\langle 1 + 2\omega,\ 3 + 3\omega \pmod{\mathfrak{p}^2} \right\rangle,$$

where, $(1+2\omega)^2 \equiv (3+3\omega)^6 \equiv 1 \pmod{\mathfrak{p}^2}$ *of type* $(2,6)$,

$$\nu = \left\langle 3+3\omega \pmod{}p^2 \right\rangle,$$

(ii) *If* $c \equiv 3 \pmod 4$, *then*

$$\alpha = \left\langle -1,\ -\omega \pmod{\mathfrak{p}^2} \right\rangle,$$

where, $(-1)^2 \equiv (-\omega)^6 \equiv 1 \pmod{\mathfrak{p}^2}$ *of type* $(2,6)$,

$$\nu = \left\langle -\omega \pmod{}p^2 \right\rangle,$$

(2) *if* $dn \equiv 1 \mod 8$, $dm \equiv 2 \pmod 4$, *then*

$$D_{K/k} = 4m,\ 2 = \mathfrak{p}\mathfrak{p}',\ \mathfrak{p} = (2,\omega),\ r = 3,\ \varphi_k(\mathfrak{p}^3) = 4,$$

$$\alpha = \left\langle 3,\ 7 \pmod{\mathfrak{p}^3} \right\rangle,$$

where, $3^2 \equiv 7^2 \equiv 1 \pmod{\mathfrak{p}^3}$ and

$$\nu = \left\langle 1-mn \pmod{\mathfrak{p}^3} \right\rangle.$$

We can obtain the same results for $\mathfrak{p}' = \left(2,\ \frac{1-\sqrt{dn}}{2}\right)$,

$(2)'$ *if* $dn \equiv 5 \pmod 8$, $dm \equiv 2 \pmod 4$, *then*

$$D(K/k) = 4m,\ 2 = \mathfrak{p},\ r = 3,\ \varphi_k(\mathfrak{p}^3) = 48,$$

$$\alpha = \left\langle -3,\ 1+4\omega,\ c-dm+\omega \pmod{\mathfrak{p}^3} \right\rangle,$$

$(-3)^2 \equiv (1+4\omega)^2 \equiv (c-dm+\omega)^{12} \equiv 1 \pmod{\mathfrak{p}^3}$ *of type* $(2,2,12)$,

$$\nu = \left\langle -3,\ c-dm+\omega \pmod{\mathfrak{p}^3} \right\rangle,$$

(3) *if* $dn \equiv 3$, $dm \equiv 2 \pmod 4$, *then we have*

$$D(K/k) = 2m,\ 2 = \mathfrak{p}^2,\ \mathfrak{p} = (2, 1+\sqrt{dn}),\ r = 4,\ \varphi_k(\mathfrak{p}^4) = 8,$$

$$\alpha = \left\langle 1+2\sqrt{dn},\ \sqrt{dn} \pmod{\mathfrak{p}^4} \right\rangle$$

$(1+2\sqrt{dn})^2 \equiv \sqrt{dn}^4 \equiv 1 \pmod{\mathfrak{p}^4}$ *of type* $(2,4)$,

$$\nu = \left\langle \sqrt{dn} \pmod{\mathfrak{p}^4} \right\rangle,$$

$(3)'$ *if* $dn \equiv 2$, $dm \equiv 3 \pmod 4$, *then we have*

$$D(K/k) = 2m,\ 2 = \mathfrak{p}^2,\ \mathfrak{p} = (2, \sqrt{dn}),\ r = 2,\ \varphi_k(\mathfrak{p}^2) = 2,$$

$$\alpha = \left\langle 1 + \sqrt{dn} \pmod{\mathfrak{p}^2} \right\rangle,$$

where, $(1+\sqrt{dn})^2 \equiv 1 \pmod{\mathfrak{p}^2}$.

$$\nu =< 1 >,$$

(4) *if* $dn \equiv dm \equiv 2,\ \prod q_1 \prod q_2 \equiv 3 \pmod 4$, *then the result are the same as one of the case* $(3)'$ *because we may assume that* K *is equal to one of* $(3)'$.

Proof. We may verify that the group of the norm residues $\{\nu \in k\ ;\ \nu \equiv N_{K/k}(\Gamma) \pmod{\mathfrak{p}^r}, \Gamma \in K, (\nu, \mathfrak{p}) = 1\}$ is given by Theorem 2.3 because we can give other parts $D(K/k),\ \varphi(\mathfrak{p}^r)$ and α, directly.

In the cases (1) , (2) and $(2)'$, we can use Z_K of Theorem 2.1 (2) and (3.1). By making a permutation $\begin{pmatrix} d & m & n \\ m & n & d \end{pmatrix}$ in these cases, we have the following integral basis of Z_K;

$$Z_K = \boldsymbol{Z}\left[1, \frac{1+\sqrt{dn}}{2}, \sqrt{dm}, \frac{\sqrt{mn}+\sqrt{dm}}{2}\right].$$

Put

$$A = x + y\frac{1+\sqrt{dn}}{2} + z\sqrt{dm} + w\frac{\sqrt{mn}+\sqrt{dm}}{2},$$

where, x, y, z and w are rational integers.

Then, we have $N_{K/k}A = a + b\omega$, where a and b are rational integers with

$$a = x^2 + cy^2 - mnz\left(z + \frac{w}{2}\right) - dm\frac{w^2}{2},$$

$$b = y^2 + 2xy \mp mw\left(z + \frac{w}{2}\right),$$

where, double signs take positive if and only if $d < 0$ and $n < 0$.

(1) If $dn \equiv 1, dm \equiv 3 \pmod 4$, and moreover

(i) if $c \equiv 1 \pmod 4$, then we put $x = y = z = 1,\ w = 0$.

Then we obtain $a \equiv b \equiv 3 \pmod 4$, and hence $3 + 3\omega$ is a norm residue for molulo $\mathfrak{p}^2$. Thus ν is equal to a cyclic group $< 3 + 3\omega \pmod{\mathfrak{p}^2} >$.

(ii) If $c \equiv 3 \pmod 4$, then we put $x = y = 1,\ z = -2,\ w = 4$.

Then we obtain $a \equiv 0,\ b \equiv 3 \pmod 4$, and hence 3ω is a norm residue for modulo $\mathfrak{p}^2$. Thus ν is equal to a cyclic group $< 3\omega \pmod{\mathfrak{p}^2} >$.

(2) If $dn \equiv 1 \pmod 8, dm \equiv 2 \pmod 4$, then we put $x = z = 1,\ y = w = 0$. Then we obtain $b = 0,\ a = 1 - dm$. Thus ν is equal to a cyclic group $< 1 - mn \pmod{\mathfrak{p}^3} >$.

(2)′ If $dn \equiv 5 \pmod 8, dm \equiv 2 \pmod 4$, then first we put $x = 1,\ y = z = 0,\ w = 4$. Then we obtain $b \equiv 0,\ a \equiv 1 - 4mn \equiv -3 \pmod 8$. Thus $-3 \pmod{\mathfrak{p}^3}$ is a norm residue. Next Put $x = 0,\ y = 1,\ z = -1,\ w = 2$. Then we obtain $a = c - dm,\ b = 1$. Thus $c - dm + \omega \pmod{\mathfrak{p}^3}$ is a norm residue. Therefore we have
$\nu =< -3,\ c - dm + \omega \pmod{\mathfrak{p}^3} >$.

we have the following integral basis of Z_K;

$$Z_K = \boldsymbol{Z}\left[1, \sqrt{dn}, \sqrt{dm}, \frac{\sqrt{dm} + \sqrt{mn}}{2}\right].$$

Put

$$A = x + y\sqrt{dn} + z\sqrt{dm} + w\frac{\sqrt{dm} + \sqrt{mn}}{2},$$

where, x, y, z and w are rational integers. Then we have $N_{K/k}A = a + b\sqrt{dn}$,
where, a and b are rational integers with

$$a = x^2 + dny^2 - dmz(z + w) - \frac{1}{4}dn(d + n)mw^2,$$

$$b = 2xy \mp \frac{1}{2}mw(w + 2z).$$

Here, double signs take positive if and only if $m < 0$ and $n < 0$.

Put $x = y = w = 1$, then we obtain

$$a \equiv z(1 + z) - \frac{d + n}{2},\ b \equiv 2(1 + z) \mp 1 \pmod 4.$$

From these relations with respect to z, we see that congruence equation
$a \equiv 0 \pmod 4,\ b \equiv 1 \pmod 2$ is solvable. On the other hand we have

$$\sqrt{dn}^{\,2} \equiv dn \equiv 3 \pmod 4 \text{ and } (\alpha : \nu) = 2.$$

Therefore $\sqrt{dn}$ is a norm residue for modulo $\mathfrak{p}^4$. Thus ν is equal to a cyclic group $< \sqrt{dn} \pmod{\mathfrak{p}^4} >$.

Finally we consider the case (3)′. We can use Z_K of Theorem 2.1 (3.2). By making a transposition $(d\ n)$ in this case, we have the following integral basis of Z_K;

$$Z_K = \boldsymbol{Z}\left[1, \sqrt{dm}, \sqrt{mn}, \frac{\sqrt{mn}+\sqrt{dn}}{2}\right].$$

$$A = x + y\sqrt{dm} + z\sqrt{mn} + w\frac{\sqrt{mn}+\sqrt{dn}}{2},$$

where, x, y, z and w are rational integers. Then we have $N_{K/k}A = a + b\sqrt{dn}$, where, a and b are rational integers with

$$a = x^2 + dn\left(\frac{w^2}{2}\right) - dmy^2 - mn\left(z + \frac{w}{2}\right)^2,$$

$$b = xw \mp my(2z + w).$$

Here, double signs take positive if and only if $d < 0$ and $n < 0$.

Put $x = 0,\ y = 1,\ z = -1,\ w = 2$, then we obtain

$b = 0,\ a \equiv dn - dm \equiv d(n - m) \equiv 1 \pmod 2$. Therefore 1 is a norm residue for modulo 2, i.e., for modulo $\mathfrak{p}^2$. Thus ν is equal to the unit group $< 1 >$. Therefore we have proved Theorem 2.3 completely. ∎

3. On a Problem of Hasse for Certain Imaginary Abelian Fields

3.1. Introduction. Let K be an algebraic number field over the rationals $\boldsymbol{Q}$. If the ring $Z_K = \boldsymbol{Z}[\theta]$ of integers in K is generated by an integer θ over the ring $\boldsymbol{Z}$ of rational integers, it is said that Z_K has a power basis, Z_K is monogenic or of monogenesis, otherwise Z_K is said to be non-monogenic or of non-monogenesis.

Let k_n be an n-th cyclotomic field $\boldsymbol{Q}(\zeta_n)$ over $\boldsymbol{Q}$ and k_n^+ the maximal real subfield of k_n, where ζ_n be a primitive n-th root of unity. In [Gr_1, Gr_2] M.-N. Gras showed the non-monogenesis of the ring Z_K of integers in cyclic fields K over $\boldsymbol{Q}$ of prime degrees $\ell \geq 5$ except for $K = k_{2l+1}^+$, where $2\ell + 1$ is a prime, and subsequently, she proved that there exist only finitely many abelian extensions K over $\boldsymbol{Q}$ of degrees $m \geq 5$, $(m, 6) = 1$, whose Z_K have a power basis using the prime decomposition of Gauß sum by H. W. Leopoldt [Le].

In Theorem 3.1, we shall give a new family of infinitely many imaginary abelian fields K of degrees $m > 2$ whose rings Z_K are of non-monogenesis applying some evaluation of the different of a number in K [Lemma 3.1]. In Theorem 3.2, we shall characterize infinitely many imaginary abelian fields K of degrees $m > 2$ whose rings Z_K are of monogenesis using Lemma 3.2.

3.2. Non-Monogenic Phenomena For Abelian Extensions. The following lemma is fundamental for us.

Lemma 3.1. *Let f be the conductor of a cyclotomic field k_f, $\prod_p p^e$ be its canonical decomposition and σ be an element of the Galois group G of k_f over $\boldsymbol{Q}$ which generates the Galois subgroup of k_{p^e} over $\boldsymbol{Q}$. Then for any integer R of k_f, $R - R^\sigma$ is divisible by a prime element π_p in k_{p^e} for $\pi_p = 1 - \zeta_{p^e}$.*

Proof. Since p^e and f/p^e are prime to each other, there exist primitive roots ζ_{p^e} and ζ_{f/p^e} such that $\zeta_f = \zeta_{p^e}\zeta_{f/p^e}$. Then ${\zeta_f}^\sigma = \zeta_{p^e}^\sigma \zeta_{f/p^e}$. Now a number R in Z_{k_f} is

presented by a form $\sum_{1\leq j\leq n} a_j\zeta_f^j$ with $a_j \in \boldsymbol{Z}$, where n is equal to the value of the Euler function $\varphi(f)$. Then $R - R^\sigma = \sum_{1\leq j\leq n} a_j(\zeta_{p^e}^j - \zeta_{p^e}^{j\sigma})\ \zeta_{f/p^e}^j$. Since $\zeta_{p^e}^j - \zeta_{p^e}^{j\sigma}$ is divisible by π_p for any $\varrho \in G$, $R - R^\sigma$ is divisible by π_p. ∎

Theorem 3.1. *Let K be the composite field of an imaginary quadratic field $\boldsymbol{Q}(\omega)$ and a real abelian field L distinct from the rationals $\boldsymbol{Q}$, whose conductors are prime to each other.*

(1) *If $\boldsymbol{Q}(\omega) \neq \boldsymbol{Q}(i)$ with $i^2 = -1$, then Z_K is of non-monogenesis,*

(2) *If $\boldsymbol{Q}(\omega) = \boldsymbol{Q}(i)$, then for a sextic field K, Z_K is of non-monogenesis except for two fields of conductors* 28 *and* 36.

Proof. Let τ be the generator of Galois group of $\boldsymbol{Q}(\omega)$ over $\boldsymbol{Q}$ and H the Galois group of L over $\boldsymbol{Q}$. Let $d(K)$ and $d(\xi)$ be the field discriminant of K and the discriminant of a number ξ in K, respectively. Then a ring Z_K is of monogenesis if and only if there exists a number ξ in K such that $|d(\xi)| = |d(K)|$. Now put $H^* = H \setminus \{e\}$, where e is the identity in H. Since the Galois group of K over $\boldsymbol{Q}$ is generated by τ and H, we have

$$\begin{aligned} |d(\xi)| &= |(N_K \prod_{\sigma\in H^*}(\xi - \xi^\sigma))(N_K(\xi - \xi^\tau))(N_K \prod_{\sigma\in H^*}(\xi - \xi^{\tau\sigma}))| \\ &= |d(K)||N_K\alpha||N_K \prod_{\sigma\in H^*}(\xi - \xi^{\tau\sigma}))| \end{aligned}$$

for some integer α in K. Therefore if Z_K is of monogenesis, $|N_K \prod_{\sigma\in H^*}(\xi - \xi^{\tau\sigma})| = 1$ should be held. We assume that such ξ exists. Let $\prod_p p^e$ be the canonical decomposition of the conductor f of L. Then an f-th root ζ_f of unity can be written as $\prod_p \zeta_{p^e}$ for some p^e-th root ζ_{p^e} of unity. Let A be the subgroup of the Galois group G_f of k_f over $\boldsymbol{Q}$, which corresponds to the subfield L of k_f. The group H is isomorphic to the factor group G_f/A. Denote the Galois group of k_{p^e} over $\boldsymbol{Q}$ by A_p with a generator σ_p. Then we have a direct product decomposition $\prod_p A_p$ of G_f. Every σ_p is not contained in A, namely $\overline{\sigma}_p \in H^*$. Because if the group A contains some σ_p, we

have $H \cong G_f/A \cong (G_f/ < \sigma_p >)/(A/ < \sigma_p >)$, where $< \varrho >$ for $\varrho \in G$ denotes the subgroup of G generated by ϱ. This contradicts to the conductor f of L.

First, we consider the case where $Q(\omega)$ has an odd conductor m. Then $\boldsymbol{Q}(\omega) = \boldsymbol{Q}(\sqrt{-m})$ and $\{\omega, \omega^\tau\}$ for $\omega = (-1+\sqrt{-m})/2$ is an integral basis of $Z_{\boldsymbol{Q}(\omega)}$. Since we can put $\xi = \omega R + \omega^\tau S$ for some $R, S \in Z_L$ by [La], it holds that for $\sigma \in H^*$,

$$\begin{aligned}(\xi - \xi^{\tau\sigma})(\xi^\tau - \xi^\sigma) &= \{\omega(R - S^\sigma) + \omega^\tau(S - R^\sigma)\}\{\omega(S - R^\sigma) + \omega^\tau(R - S^\sigma)\} \\ &= \omega\omega^\tau\left(s_\sigma^2 + t_\sigma^2\right) + \left\{\omega^2 + (\omega^\tau)^2\right\} s_\sigma t_\sigma \\ &= \frac{1+m}{4}\left(s_\sigma^2 + t_\sigma^2\right) - \frac{m-1}{2} s_\sigma t_\sigma,\end{aligned}$$

where $s_\sigma = R - S^\sigma, t_\sigma = S - R^\sigma$. If $t_\sigma = 0$, then we have $\xi - \xi^{\tau\sigma} = \omega(R - R^{\sigma^2})$, which is divisible by a prime factor π_p of p in L by Lemma 3.1. Thus $|d(\xi)| > |d(K)|$ holds. If $s_\sigma = 0$, we have the same conclusion. Next, assume $s_\sigma t_\sigma \neq 0$. Then it follows that

$$\begin{aligned}\tfrac{1+m}{4}(s_\sigma^2 + t_\sigma^2) - \tfrac{m-1}{2} s_\sigma t_\sigma &= |s_\sigma t_\sigma| \left\{ \frac{1+m}{4}\left(\left|\frac{s_\sigma}{t_\sigma}\right| + \left|\frac{t_\sigma}{s_\sigma}\right|\right) \mp \frac{m-1}{2} \right\} \\ &\geq |s_\sigma t_\sigma| \left\{ \frac{1+m}{2} \mp \frac{m-1}{2} \right\} \\ &\geq |s_\sigma t_\sigma|,\end{aligned}$$

where each equality holds if and only if $s_\sigma = t_\sigma$. Then we obtain $|N_L((\xi - \xi^{\tau\sigma})(\xi^\tau - \xi^\sigma))| \geq |N_L s_\sigma t_\sigma|$. If $s_\sigma \neq t_\sigma$, we have $|N_L((\xi - \xi^{\tau\sigma})(\xi^\tau - \xi^\sigma))| > 1$, namely $|d(\xi)| > |d(K)|$. If $s_\sigma = t_\sigma$, then we have $\xi - \xi^{\tau\sigma} = (\omega + \omega^\tau)(R - S^\sigma) = -(R - S^\sigma) = -(S - R^\sigma)$ $= -\frac{1}{2}\{(R+S) - (R+S)^\sigma\}$ which contains a prime factor π_p of p. Then $|d(\xi)| > |d(K)|$.

Secondly, we treat the case where $\boldsymbol{Q}(\omega)$ has an even conductor $m > 1$. Then $\boldsymbol{Q}(\omega) = \boldsymbol{Q}(\sqrt{-m})$ and $\{1, \omega\}$ for $\omega = \sqrt{-m}$ is an integral basis of $Z_{\boldsymbol{Q}(\omega)}$. Since we can put $\xi = R + \omega S$ for some $R, S \in Z_L$, it holds that $\xi - \xi^\tau = 2\omega S$. Then a number S should be a unit of L. By $\xi - \xi^{\tau\sigma} = R - R^\sigma + \omega(S + S^\sigma)$, if $S + S^\sigma = 0$, then $\xi - \xi^{\tau\sigma}$ is divisible by a prime factor π_p of p. Hence $|d(\xi)| > |d(K)|$. If $S + S^\sigma \neq 0$, then $(\xi - \xi^{\tau\sigma})(\xi^\tau - \xi^\sigma) \geq m(S + S^\sigma)^2$. Thus we have

$$|N_K(\xi - \xi^{\tau\sigma})| \geq |N_L m(S + S^\sigma)^2| \geq m^{[L\,:\,\boldsymbol{Q}]} > 1.$$

Then $|d(\xi)| > |d(K)|$.

Finally, we consider the case where $\boldsymbol{Q}(\omega)$ coincides with the Gauß field $\boldsymbol{Q}(i)$ and L is a cubic subfield of k_f of an odd conductor f.

Then we have $H = \{e, \sigma, \sigma^2\}$. For $\varrho \in H$, it holds that

$$(\xi - \xi^{\tau\varrho})(\xi^{\tau} - \xi^{\varrho}) = (R - R^{\varrho})^2 + (S + S^{\varrho})^2.$$

If $S + S^{\varrho} = 0$, Then $R - R^{\varrho}$ is divisible by a prime factor π_p in L, where p^e is a prime power factor of f. Here we can consider a presentative ϱ as an automorphism $\neq e$ of k_{p^e} over $\boldsymbol{Q}$. Then we may assume $S + S^{\varrho} \neq 0$. If $R - R^{\varrho} \neq 0$ for some $\varrho \in H$, then it holds that $(R - R^{\varrho})^2 + (S + S^{\varrho})^2 \geq 2|(R - R^{\varrho})(S + S^{\varrho})|$. Then it follows that $|N_K(\xi - \xi^{\tau\varrho})| \geq |N_L 2(R - R^{\varrho})(S + S^{\varrho})| \geq 8$. Next, let $R - R^{\varrho} = 0$ for any $\varrho \in H$, namely $R \in \boldsymbol{Z}$. Then $\xi - \xi^{\tau\varrho} = i(S + S^{\varrho})$. Hence if a number ξ generates a power basis of Z_K, the number $S + S^{\varrho}$ should be a unit of L, that is

$$N_L(S + S^{\varrho}) = (S + S^{\varrho})(S^{\varrho} + S^{\varrho^2})(S^{\varrho^2} + S) = \pm 1.$$

On the other hand, as the same evaluation as in the second case, $N_L S = S S^{\varrho} S^{\varrho^2} = \pm 1$ holds. Put $s_1 = S + S^{\varrho} + S^{\varrho^2}$, $s_2 = S S^{\varrho} + S^{\varrho} S^{\varrho^2} + S^{\varrho^2} S$. Then it holds that

$$\begin{aligned} N_L(S + S^{\varrho}) &= (s_1 - S^{\varrho^2})(s_1 - S)(s_1 - S^{\varrho}) \\ &= s_1^3 - s_1^2 s_1 + s_1 s_2 \mp 1 = s_2 s_1 \mp 1 = \pm 1. \end{aligned}$$

Then we have two cases of (i) $s_1 s_2 = 0$ or (ii) $s_1 s_2 = \pm 2$.

(i) If $s_1 = 0$, then a number S is a solution of $x^3 + s_2 x \pm 1 = 0$. Thus $-d(S) = 4s_2^3 + 27$. Since the field discriminant $d(L)$ is equal to f^2, we have $(fa)^2 = -4s_2^3 - 27$, namely $(4fa)^2 = (-4s_2)^3 - 432$. By the tranformation $x = \frac{12}{u+v}, y = \frac{36(u-v)}{u+v}$, the diophantine equation $y^2 = x^3 - 432$ is birationally equivalent to the Fermat curve $u^3 + v^3 = 1$, whose solutions are of $(\pm 36)^2 = 12^3 - 432$ [ST]. Then $f = 3^2, s_2 = -3$. Thus the solutions of the equation $x^3 - 3x + 1 = 0$ are $S = \zeta_9 + \zeta_9^{-1}$ and its conjugates. If $s_2 = 0$, the numbers $\pm 1/S$ are solutions of the same equation as in the case of $s_1 = 0$. Therefore the field L coincides with the maximal real subfield k_9^+ of conductor 3^2. Then we obtain $Z_K = \boldsymbol{Z}[iS]$ for $S = \zeta_9 + \zeta_9^{-1}$.

(ii) If $s_1 s_2 = \pm 2$, noting the signature of $N_L(S + S^\sigma)$ coincides with the product of ones of s_1 and s_2, a number S is a solution of one of the following eight cases;

$$\begin{array}{ll} x^3 - x^2 + 2x - 1 = 0,\ d(S) = -23, & x^3 - x^2 - 2x + 1 = 0,\ d(S) = 49, \\ x^3 + x^2 + 2x + 1 = 0, & x^3 + x^2 - 2x - 1 = 0, \\ x^3 - 2x^2 + x - 1 = 0, & x^3 - 2x^2 - x + 1 = 0, \\ x^3 + 2x^2 + x + 1 = 0, & x^3 + 2x^2 - x - 1 = 0. \end{array}$$

Each of latter six equations is obtained from one of the former two ones by a linear fractional transformation. Since the discriminant $d(S)$ of a number S in a cyclic cubic field L must be square, we have a solution $S = \zeta_7 + \zeta_7^{-1}$ of $x^3 + x^2 - 2x - 1 = 0$, which generates the maximal real subfield k_7^+ of conductor 7. Then we obtain $Z_K = \boldsymbol{Z}[iS]$. Therefore we have proved the theorem. ∎

Remark 3.1. In two cases of the maximal imaginary sextic subfields K of conductors 28 and 36 in k_{28} and k_{36}, the proof of Theorem 3.1 (2) involves that there are generators $\pm iS, \pm i/S$ and their conjugates only for Z_K except for the parallel transformations of them by rational integers. For the cases of cyclotomic fields k_p of the prime conductor p, $p \leq 23, p \neq 17$, L. Robertson completely determined the generators of Z_{k_p} in [Ro$_1$].

Remark 3.2. Let p be an odd prime number greater than three, $n = 3p^m$ and k_n be an n-th cyclotomic field $\boldsymbol{Q}(\zeta_n)$ over the rationals $\boldsymbol{Q}$, where ζ_n be a primitive n-th root of unity. Let K^- be the imaginary subfield of k_n with $[k_n : K^-] = 2$, which is different to $k_{n/3}$. Then it has been shown that the ring Z_{K^-} of integers has no power basis [SN$_2$].

By [Sh], it is given a necessary and sufficient condition Z_K having a power basis for a cyclic sextic field K of a prime conductor, and a problem and a conjecture are proposed as follows;

Problem. *Is there no cyclic sextic field K of a prime conductor $p \equiv 1 \pmod 6$ whose ring Z_K of integers is monogenic except for the cyclotomic field k_7 of conductor 7 and the maximal real subfield of k_{13} of conductor 13?*

Conjecture. *Let p be a prime number and put $m = 3p$ $(p \neq 3)$, $4p$ $(p \neq 7)$ or $m \neq 36$. Then there exists a subfield K of k_m with $[K : \boldsymbol{Q}] = 6$ whose ring Z_K of integers does not have a power basis.*

The conjecture above has been solved in general by Theorem 3.1.

3.3 Monogenic Phenomena for Abelian Extensions. Let K be the composite field of $\boldsymbol{Q}(i)$ and any real subfield L distinct from $\boldsymbol{Q}$ of an odd conductor $f > 1$ of k_f. Assume that the ring Z_K of integers in K has a power basis, that is $|d(\xi)| = |d(K)|$ for some $\xi = R + iS \in Z_K$, where $R, S \in Z_L$. Then we can see that $R \in \boldsymbol{Z}$, and S, $S + S^{\varrho}$ are units of L for $\varrho \in H^*$. We have $\xi - \xi^{\varrho} = i(S - S^{\varrho})$. Hence by assumption, it holds that

$$|N_K \prod_{\varrho \in H^*} (\xi - \xi^{\varrho})| = |N_L(S - S^{\varrho})|^2 = d(L)^2.$$

Then $Z_L = \boldsymbol{Z}[S]$, namely Z_L has a power basis. Especially, if the extension degree of the field L over $\boldsymbol{Q}$ is a prime $\ell \geq 5$, then by [Gr_2], f should be a prime of $2l + 1$, namely L is the maximal real subfield k_f^+ of k_f.

Conversely, suppose that a field k_f^+ is the maximal real subfield of k_f of an odd conductor $f > 1$ and let K be the composite field of $\boldsymbol{Q}(i)$ and k_f^+. Then it follows that the maximal real subfield K^+ of K coincides with k_f^+. Put $\xi = iS$ for units $S = \zeta + \zeta^{-1}$, $\zeta = \zeta_f$ in k_f^+. Let H be the Galois group of k_f^+ over $\boldsymbol{Q}$. Then we have for an element $\sigma \in H^*$, $\zeta^{\sigma} \neq \zeta^{\pm 1}$. Thus it follows that

$$\begin{aligned} \xi - \xi^{\tau\sigma} &= i(S + S^{\sigma}) \\ &\cong \zeta + \zeta^{-1} + \zeta^{\sigma} + (\zeta^{-1})^{\sigma} \\ &= \zeta(1 + \zeta^{\sigma-1}) + \zeta^{-\sigma}(1 + \zeta^{\sigma-1}) \\ &= \zeta^{-\sigma}(1 + \zeta^{\sigma+1})(1 + \zeta^{\sigma-1}), \end{aligned}$$

where $\alpha \cong \beta$ for $\alpha, \beta \in K$ means that $(\alpha) = (\beta)$ holds as ideals.

Lemma 3.2. *Let g be an odd number > 1 and $(a, g) = 1$. Then for a primitive g-th root ζ of unity, $1 + \zeta^a$ is a unit in a cyclotomic field k_g.*

Proof. Let $\Phi_g(X) = \prod_{d|g}(X^d-1)^{\mu(g/d)}$ be the cyclotomic polynomial of degree $\varphi(g)$, where $\varphi(\cdot)$ and $\mu(\cdot)$ means the Euler function and the Möbius one, respectively. Let $\prod_p p^e$ be the canonical decomposition of g. Then by

$$\Phi_g(X) = \Phi_{g/p^e}(Y^p)\cdot\Phi_{g/p^e}(Y)^{-1},\ Y = X^{p^{e-1}},$$

we obtain $\Phi_g(-1) = 1$, because of $\Phi_{g/p^e}(-1) \neq 1$. Then a number $1+\zeta_g^a$ is a unit in k_g for $(a,g) = 1$. ∎

By Lemma 3.2, each of $1+\zeta^{\sigma+1}$ and $1+\zeta^{\sigma-1}$ is a unit in a cyclotomic field k_g for $g|f$ and $g > 2$. Thus $|N_K \prod_{\sigma\in H^*} i(S+S^\sigma)| = 1$. Therefore Z_K is of monogenesis. Then we obtain the following theorem.

Theorem 3.2. *Let K be the composite field of the Gauß field $\boldsymbol{Q}(i)$ and a real subfield L of an odd conductor $f > 1$ of k_f. Assume that the ring Z_K of integers in K has a power basis, then the ring Z_L of integers in L has also a power basis. Conversely, let L be the maximal real subfield of k_f of an odd conductor $f > 1$ and K be the composite field of $\boldsymbol{Q}(i)$ and L. Then the ring Z_K of integers in K has a power basis.*

As an application of Theorem 3.2 to [Gr$_2$] we obtain

Corollary 3.1. *Let ℓ be a prime number congruent to 7 modulo 30 and $\ell > 7$. Then there exist infinitely many abelian fields K of conductor 4ℓ whose integer rings Z_K have no power basis.*

Proof. Choose a proper subfield $\neq \boldsymbol{Q}$ of k_ℓ^+ as a field L in the above theorem and K be the composite field of $\boldsymbol{Q}(i)$ and L. Then by Theorem 3.2 and [Gr$_2$], the ring Z_K has no power basis. ∎

Remark 3.3. On the former part of Theorem 3.2, by [Gr$_2$] if the conductor f of L is a prime such that $f = 2\ell+1$, where ℓ is also a prime ≥ 5 and $[L:\boldsymbol{Q}] \geq 5$, then the field L coincides with the maximal real subfield k_f^+.

4. Power Integral Bases in Algebraic Number Fields whose Galois Groups are 2-elementary Abelian

4.1. Introduction. M.-N. Gras determined that any cyclic extension $K/\boldsymbol{Q}$ of prime degree $\ell \geq 5$ is non-monogenic except for the maximal real subfield $\boldsymbol{Q}^+(\zeta_f)$ of an f-th cyclotomic field $\boldsymbol{Q}(\zeta_f)$, where $f = 2\ell+1$ is a prime and ζ_n is an n-th primitive root of unity[G]. Further M.-N. Gras and F. Tanoé gave a necessary and sufficient condition for monogenesis of biquadratic fields by using a diophantine equation of degree 4 [GT] and a new family of infinitely many monogenic biquadratic fields was constructed by the first author [M_2].

Let $\boldsymbol{Z}$ be the ring of rational integers and let Z_F be the ring of integers in an algebraic number field F over the rationals $\boldsymbol{Q}$. It is called that Z_F has a power integral basis or F is monogenic when Z_F is generated by an integer θ as the ring $\boldsymbol{Z}[\theta]$.

In this paper, we treat Hasse's problem, that is, we will characterize whether a field F is monogenic or not in some family of the 2-elementary abelian extensions.

Let F be a field over the rationals $\boldsymbol{Q}$ whose Galois group is 2-elementary abelian. If $[F : \boldsymbol{Q}] \geq 16$, then F is non-monogenic, i.e., Z_F has no power integral basis by virtue of the decomposition theory of a prime number (Proposition 4.2). In the octic case of $[F : \boldsymbol{Q}] = 8$, by Proposition 4.3 it is enough for us to investigate the field $F = \boldsymbol{Q}\left(\sqrt{mn}, \sqrt{dn}, \sqrt{\ell}\right)$, where dmn and ℓ are square-free, $mn \equiv 3, \ell \equiv 1, d \equiv 2, \pmod 4, d > 0$.

In this paper, we assume $(dmn,\ \ell) = 1$. Then we will claim that any real 2-elementary abelian field has no power integral basis and a complex one has a power integral basis only if it coincides with $\boldsymbol{Q}\left(\sqrt{-1}, \sqrt{-2}, \sqrt{-3}\right)$, namely the 24-th cyclotomic field $\boldsymbol{Q}(\zeta_{24})$.

4.2. General cases and preliminaries. We consider fields F whose Galois groups are 2-elementary abelian. We will show that if $[F : \boldsymbol{Q}] \geq 16$, then F is non-monogenic.

So it is enough for us to consider the case $[F : \boldsymbol{Q}] = 8$ and we give a necessary condition that F is monogenic (Proposition 4.3).

Proposition 4.1. *Let* $a_1, a_2, \cdots, a_r$ *be square-free rational integers and* F *be the field* $\boldsymbol{Q}\left(\sqrt{a_1}, \cdots, \sqrt{a_r}\right)$ *of degree* 2^r, $r \geq 2$. *Then it is deduced that there exists at most one* i *and* j *such that* $a_i \equiv 3$, $a_j \equiv 2 \pmod 4$, *respectively.*

Proof. By $\boldsymbol{Q}(\sqrt{a_1}, \sqrt{a_2}) = \boldsymbol{Q}(\sqrt{a_1}, \sqrt{a_1 a_2})$, this proposition follows. ∎

Lemma 4.1 ([SN_2]). *Let* ℓ *be a prime number and let* $K/\boldsymbol{Q}$ *be Galois extension of degree* $n = efg$ *with the ramification index* e *and the relative degree* f *with respect to* ℓ. *If one of the following conditions is satisfied, then* Z_K *has no power integral basis, i.e.,* K *is non-monogenic* ;

(1) $e\ell^f < n$ *if* $f = 1$,

or

(2) $e\ell^f \leq n + e - 1$ *if* $f \geq 2$.

Proposition 4.2. *If* $r \geq 4$ *for* $F = \boldsymbol{Q}\left(\sqrt{a_1}, \cdots, \sqrt{a_r}\right)$, *then* F *is non-monogenic.*

Proof. By Proposition 4.1, the ramification index with respect to the place 2 is at most 4 in $F/\boldsymbol{Q}$. Since the Galois group $G = Gal(F/\boldsymbol{Q})$ is 2-elementary, the relative degree f of the prime 2 is at most 2. Let ℓ be equal to 2 in Lemma 4.1. Then it follows that $e\ell^f \leq 2^2 \cdot 2^1 < 2^r$ if $f = 1$, and $e\ell^f \leq 2^2 \cdot 2^2 \leq 2^r + e - 1$ if $f = 2$. Therefore F is non-monogenic by Lemma 4.1. ∎

Proposition 4.3. *Let* $F = \boldsymbol{Q}\left(\sqrt{mn}, \sqrt{dn}, \sqrt{d_1 m_1 n_1 \ell}\right)$ *with an odd* mn, $d > 0$, $d_1 | d$, $m_1 | m$, $n_1 | n$, $d_1 m_1 n_1 \ell \equiv 1 \pmod 4$ *and* $dmn\ell$ *is square-free. If* F *is monogenic, then the ramification index* e *with respect to the place* 2 *is equal to* 4, *i.e., we have* $mn \equiv 3$, $d \equiv 2 \pmod 4$.

Proof. Since the order f of the inert group is at most 2, if e is equal to 2, we have $e\ell^f = 2 \cdot 2^1 < 8$ or $e\ell^f = 2 \cdot 2^2 < 8 + 2 - 1$. Then F is non-monogenic by Lemma 4.1. ∎

Remark 4.1. M.-N. Gras and F. Tanoé gave a necessary and sufficient condition that the ring of integers in a biquadratic field $K = \boldsymbol{Q}(\sqrt{mn}, \sqrt{dn})$ has a power basis, i.e., K is monogenic as follows[GT];

(1) in the case $dm \equiv dn \equiv 2,\ mn \equiv 1 \pmod 4$ or $dm \equiv dn \equiv 3 \pmod 4$, and $m - n = 4d$, the equation $(u^2 - v^2)^2 m - (u^2 + v^2)^2 n = \pm 4$ has a solution $\{u, v\}$ in $\boldsymbol{Z}$, or

(2) in the case $dm \equiv dn \equiv 2,\ mn \equiv 3 \pmod 4$, and $m - n = d$, the equation $(u^2 - v^2)^2 m - (u^2 + v^2)^2 n = \pm 2$ has a solution $\{u, v\}$ in $\boldsymbol{Z}$.

If K is monogenic, then a generator θ of Z_K is geven by

$$\theta = uv\frac{1 - \delta + 2^\delta\sqrt{mn}}{2} + v^2\sqrt{dn} + (u^2 - v^2)\frac{\sqrt{dm} + \sqrt{dn}}{2},$$

with $\delta = 0$ or 1 and $mn \equiv (-1)^\delta \pmod 4$.

The first author proved that there exists infinitely many real monogenic biquadratic fields for any relatively prime fixed pair $\{u,\ v\}$ with parameters $d,\ m,\ n$ and gave a method of construction of them [M_2].

Therefore we restrict ourselves to consider the case of octic extension $[F : \boldsymbol{Q}] = 8$.

Proposition 4.4. *Let* $F = \boldsymbol{Q}\left(\sqrt{mn}, \sqrt{dn}, \sqrt{d_1 m_1 n_1 \ell}\right)$ *with* $d_1|d,\ m_1|m,\ n_1|n,$ $mn \equiv 3,\ d_1 m_1 n_1 \ell \equiv 1,\ d \equiv 2 \pmod 4, d > 0$ *and* $dmnl$ *is square free. Then we have* $D(F) = 2^{12}(dmn\ell)^4$.

Proof. Let p be a ramified prime number in F. We evaluate the exponent r of any prime divisor $\mathfrak{P}$ of p in F of the field different $\mathfrak{d}(F/\boldsymbol{Q})$. Fisrt we consider that $\mathfrak{P}$ is tamely ramified in F. Let $\mathfrak{p}|p$ be the prime divisor in a suitable quadratic subfield k, where $\mathfrak{a}|\mathfrak{b}$ means that an ideal $\mathfrak{a}$ is a divisor of an ideal $\mathfrak{b}$ in a suitable field. Then

we have $(p) = \mathfrak{p}^2 = \mathfrak{P}^2$ in F, hence $r = e - 1 = 1$ by [CF, p.92 Lemma 6]. Let $k = \boldsymbol{Q}(\sqrt{mn})$ and $K = \boldsymbol{Q}(\sqrt{mn}, \sqrt{dn})$. Next let $\mathfrak{P}$ be wildly ramified in F. Then we have $p = 2$ and $(2) = \mathfrak{p}^2$ in k, $(2) = \mathfrak{P}^4$ in K and F, because the prime number 2 is unramified in F/K. We may assume the prime divisor $\mathfrak{P} \cap Z_K$ in K is also prime $\mathfrak{P}$ in F. Then the $\mathfrak{p}$-part of the relative different $\mathfrak{d}(k/\boldsymbol{Q})$ is equal to $\mathfrak{p}^2$ and the $\mathfrak{p}$-one of the relative different $\mathfrak{d}(K/k)$ is $\mathfrak{p}^3 = \mathfrak{P}^6$ because of the ramification index of $\mathfrak{p}$ with respect to K/k is equal to 3. Then for the $\mathfrak{P}$-part $\mathfrak{P}^r$ of the $\mathfrak{d}(F/\boldsymbol{Q})$, we have $r = 0 + 6 + 2$ because of $\mathfrak{d}(F/\boldsymbol{Q}) = \mathfrak{d}(F/K)\mathfrak{d}(K/k)\mathfrak{d}(k/\boldsymbol{Q})$. Thus we obtain

$$D(F) = \mathrm{N}_F(\mathfrak{d}(F/\boldsymbol{Q})) = \prod_{\mathfrak{P}|\mathfrak{d}(F/\boldsymbol{Q})} \mathrm{N}_F(\mathfrak{P}^r) = \prod_{\mathfrak{P}|2} \mathrm{N}_F(\mathfrak{P}^8) \prod_{\mathfrak{P} \not| 2} \mathrm{N}_F(\mathfrak{P}) = 2^{16} \left(\frac{dmn\ell}{2}\right)^4.$$

Here $\mathrm{N}_F(\mathfrak{A})$ means the norm of an ideal $\mathfrak{A}$ of F with respect to $F/\boldsymbol{Q}$. ∎

4.3. The case $\mathbf{d_1 m_1 n_1 = 1}$. From now on, we consider the case of $d_1 m_1 n_1 = 1$ and we assume that F is monogenic. Denote the Galois group

$$Gal(F/\boldsymbol{Q}) = \left\langle \tau, \rho, \sigma;\ \sqrt{dm}^{\,\tau} = -\sqrt{dm},\ \sqrt{dn}^{\,\rho} = -\sqrt{dn},\ \sqrt{\ell}^{\,\sigma} = -\sqrt{\ell} \right\rangle$$

by G.

Let ξ be a generator of a power integral basis of F. Then we have the identity,

$$(\xi - \xi^\tau)(\xi - \xi^\tau)^\rho - (\xi - \xi^\rho)(\xi - \xi^\rho)^\tau - (\xi - \xi^{\tau\rho})(\xi - \xi^{\tau\rho})^\rho = 0.$$

Let $\eta_1 = (\xi - \xi^\tau)(\xi - \xi^\tau)^\rho$. Then we show that the value of η_1 is equal to $2mE_1$ with a unit E_1 of $\boldsymbol{Q}(\sqrt{\ell})$. Since η_1 is invariant by the subgroup $< \tau,\ \rho >$, η_1 is an integer in $\boldsymbol{Q}(\sqrt{\ell})$. For the biquadratic field $K = \boldsymbol{Q}(\sqrt{dn}, \sqrt{\ell})$ fixed by the subgroup $< \tau >$ of G, the relative different $\mathfrak{d}(F/K)$ is defined by $\gcd_{\alpha \epsilon Z_F} \{\alpha - \alpha^\tau\}$. Since ξ is a generator of Z_F, $(\eta_1) = \mathfrak{d}(F/K)\mathfrak{d}(F/K)^\rho$ holds as ideals in $\boldsymbol{Q}(\sqrt{\ell})$. Since $F = K(\sqrt{mn}) = K(\sqrt{dm})$, it follows that any prime divisor $\mathfrak{Q}|m$ of F is tamely ramified in F and $\mathfrak{P}|2$ of F is wildly done in F. Then we obtain $\mathfrak{d}(F/K) = \mathfrak{P}^2 \prod_{\mathfrak{Q}|m} \mathfrak{Q}$, hence $(\eta_1) = \mathfrak{P}^4 \prod_{\mathfrak{Q}|m} \mathfrak{Q}^2 = (2m)$ by [CF]. Thus we have $\eta_1 = 2mE_1$ for a unit E_1 of $\sqrt{\ell}$. Corresponding to the second term $\eta_2 = (\xi - \xi^\rho)(\xi - \xi^\rho)^\tau$ and third $\eta_3 = (\xi - \xi^{\tau\rho})(\xi - \xi^{\tau\rho})^\rho$, since we have the biquadratic fields $\boldsymbol{Q}(\sqrt{dm}, \sqrt{\ell})$, $\boldsymbol{Q}(\sqrt{mn}, \sqrt{\ell})$ respectively, it holds that $\eta_2 = 2n(-E_2)$

and $\eta_3 = 2d(-E_3)$, for units E_j of $\boldsymbol{Q}(\sqrt{\ell})$ $(j = 2, 3)$. Then we obtain the equation (4)

$$2mE_1 \ + \ 2nE_2 \ + 2dE_3 = \ 0 \text{ in } \boldsymbol{Q}(\sqrt{\ell}).$$

In the same way, we have the following equations.

Proposition 4.5. *If* $F = \boldsymbol{Q}\left(\sqrt{mn}, \sqrt{dn}, \sqrt{\ell}\right)$ *is monogenic, then the following simultaneous equations hold* ;

(1) $$\ell E_{11} \ + \ 2dE_{12} \ + \ E_{13} \ = \ 0 \ in \ \boldsymbol{Q}(\sqrt{mn}),$$

(2) $$\ell E_{21} \ + \ E_{22} \ + \ 2mE_{23} \ = \ 0 \ in \ \boldsymbol{Q}(\sqrt{dn}),$$

(3) $$\ell E_{31} \ + \ E_{32} \ + \ 2nE_{33} \ = \ 0 \ in \ \boldsymbol{Q}(\sqrt{dm}),$$

(4) $$2dE_{41} \ + \ 2mE_{42} \ + \ 2nE_{43} \ = \ 0 \ in \ \boldsymbol{Q}(\sqrt{\ell}),$$

(5) $$2dE_{51} \ + \ E_{52} \ + \ E_{53} \ = \ 0 \ in \ \boldsymbol{Q}(\sqrt{mn\ell}),$$

(6) $$E_{61} \ + \ E_{62} \ + \ 2mE_{63} \ = \ 0 \ in \ \boldsymbol{Q}(\sqrt{dn\ell}),$$

(7) $$E_{71} + \ E_{72} \ + \ 2nE_{73} \ = \ 0 \ in \ \boldsymbol{Q}(\sqrt{dm\ell}),$$

where each of E_{ij} *is a suitable unit in the corresponding quadratic subfield of* F*, respectively.*

Proposition 4.6 ([Ri]). *Let* $\varepsilon = t + u\sqrt{D} = t + \sqrt{Du^2}$ *be a unit of a real quadratic field* $\boldsymbol{Q}(\sqrt{D})$*, and* $\varepsilon^s = t_s + u_s\sqrt{Du^2}, t_1 = t, u_1 = 1$*. Then the following properties hold* ;

(1) *If* $g = (i, j)$*, then* $(u_i, u_j) = u_g$*,*

(2) *Put* $E = \varepsilon^k = T + \sqrt{DU^2}$*, and* $E^s = T_s + U_s\sqrt{DU^2}, T_1 = T, U_1 = 1$*, then we have* $U_s = \dfrac{u_{ks}}{u_k}$.

Proof. (2) Since $U = uu_k$, we have $E^s = \varepsilon^{ks} = t_{ks} + u_{ks}\sqrt{Du^2} = t_{ks} + \frac{u_{ks}}{u_k}\sqrt{DU^2}$. Thus $U_s = \dfrac{u_{ks}}{u_k}$.

(1) Let $i = gs, j = gt$ and $(s,t) = 1$. Put $E = \varepsilon^g = t_g + u_g\sqrt{Du^2} = T + \sqrt{DU^2}$, and $E^s = T_s + U_s\sqrt{DU^2}$. Then, by (2) we have $U_s = \frac{u_{gs}}{u_g}, U_t = \frac{u_{gt}}{u_g}$. Thus
$(u_i, u_j) \equiv 0 \,(\mathrm{mod}\ u_g)$ holds. On the other hand, we have $0 < a, b \in \boldsymbol{Z}$ such that $as - bt = 1$. Then $E^1 = E^{as-bt} = (E^s)^a(E^{-t})^b$. Assume that there exixts a prime factor q of (U_s, U_t). Using $E = T + \sqrt{DU^2} = \left(T_{as} + U_{as}\sqrt{DU^2}\right)\left(T_{bt} + U_{bt}\sqrt{DU^2}\right)^{-1}$
$= \pm\left\{(T_{as}T_{bt} - U_{as}U_{bt}DU^2) + (-T_{as}U_{bt} + T_{bt}U_{as})\sqrt{DU^2}\right\}$,
and $U_{as} \equiv 0 \,(\mathrm{mod}\ U_s)$, $U_{bt} \equiv 0 \,(\mathrm{mod}\ U_t)$ it holds that $1 \equiv -T_{as}U_{bt} + T_{bt}U_{as} \equiv 0 \,(\mathrm{mod}\ q)$, which is a contradiction. ∎

In the case of a real quadratic field, the following is our key lemma.

Lemma 4.2. *Let E_j be a power $\varepsilon^j = t_j + u_j\sqrt{Du^2}$ of a unit $\varepsilon = t + \sqrt{Du^2} > 1$ in a quadratic field $\boldsymbol{Q}(\sqrt{D})$, and $\gamma \neq I$ in $Gal(\boldsymbol{Q}(\sqrt{D})/\boldsymbol{Q})$. Let*

$$\left\{\begin{array}{l} E_i a + E_j b + E_k c = 0, \\ E_i^\gamma a + E_j^\gamma b + E_k^\gamma c = 0 \end{array}\right. \tag{8}$$

for $abc \neq 0$.

Denote the matrix

$$\begin{pmatrix} E_i & E_j & E_k \\ E_i^\gamma & E_j^\gamma & E_k^\gamma \end{pmatrix}$$

attached to the equation (8) by A and the rank of A by r_D. Then we have a solution (a,b,c) of rational integers;

$$a \pm b \pm c = 0 \quad \textit{for} \quad r_D = 1,$$

$$\frac{a}{\pm U_s} = \frac{b}{\pm U_t} = \frac{c}{\pm U_u} = 1 \quad \textit{for} \quad r_D = 2,$$

with $U_v = \frac{u_{vg}}{v_g}$, $sg = j - k$, $tg = k - i$, $ug = i - j$, $(s,t,u) = 1$, $s + t + u = 0$.

Proof. First we consider the case of $r_D = 1$. Then we have

$$\frac{E_i}{E_i^\gamma} = \frac{E_j}{E_j^\gamma} = \frac{E_k}{E_k^\gamma}.$$

By taking norm for each of the denominators, we obtain $\pm E_i^2 = \pm E_j^2 = \pm E_k^2$. Since each of E_h is a real number, we have $E_i = \pm E_j = \pm E_k$, hence $a \pm b \pm c = 0$. Next assume that $r_D = 2$. The intersection of two planes $E_i a + E_j b + E_k c = 0$ and $E_i^\gamma a + E_j^\gamma b + E_k^\gamma c = 0$ with the coordinates (a,b,c) is a line which is determined

by $\frac{a}{E_jE_k^\gamma - E_kE_j^\gamma} = \frac{b}{E_kE_i^\gamma - E_iE_k^\gamma} = \frac{c}{E_iE_j^\gamma - E_jE_i^\gamma}$. Then we obtain $E_jE_k^\gamma - E_kE_j^\gamma = u_{sg}\alpha_{sg}$, $E_kE_i^\gamma - E_iE_k^\gamma = u_{tg}\alpha_{tg}$ and $E_iE_j^\gamma - E_jE_i^\gamma = u_{ug}\alpha_{ug}$ with $s+t+u=0$, where $\alpha_{vg} = \pm 2\sqrt{Du^2}$ with $N(E_{vg}) = \pm 1$. By Proposition 4.6 for $k=g$, we obtain $\pm a = \frac{u_{sg}}{u_g} = U_s$, $\pm b = \frac{u_{tg}}{u_g} = U_t$, $\pm c = \frac{u_{ug}}{u_g} = U_u$, with $(a,b,c) = 1$. ∎

Theorem 4.1. *Let F be an octic 2-elementary abelian extension $\boldsymbol{Q}\left(\sqrt{mn}, \sqrt{dn}, \sqrt{\ell}\right)$, where $mn \equiv 3, \ell \equiv 1, d \equiv 2 \pmod 4$, $d > 0$ and $dmn\ell$ is square-free. Then a field F is monogenic if and only if $F = \boldsymbol{Q}\left(\sqrt{-1}, \sqrt{-2}, \sqrt{-3}\right) = \boldsymbol{Q}(\zeta_{24})$.*

Proof. First, we consider the case that F is imaginary. Then any imaginary quadratic subfields of F are given by one of the the follwing five cases under Proposition 4.5;

$$\begin{array}{lll}
\text{(i)} & \ell < 0, m > 0,\ n > 0, & (4)\ (5)\ (6)\ (7),\\
\text{(ii)} & \ell < 0, m > 0,\ n < 0, & (1)\ (2)\ (4)\ (7),\\
\text{(iii)} & \ell < 0, m < 0,\ n < 0, & (2)\ (3)\ (4)\ (5),\\
\text{(iv)} & \ell > 0, m > 0,\ n < 0, & (1)\ (2)\ (5)\ (6),\\
\text{(v)} & \ell > 0, m < 0,\ n < 0, & (2)\ (3)\ (6)\ (7).
\end{array}$$

If F contains Gauß field $\boldsymbol{Q}(\sqrt{-1})$ and $E_1a + E_2b + E_3c = 0$ corresponds to one of the equations in Proposition 4.5, we can obtain the relation $a \pm b \pm c = 0$, since all the E_j are ± 1 or $\pm i$, because of $abc \neq 0$ for rational integers a, b, c. Since the unit group is$\{\pm 1\}$ for any other imaginary quadratic field except for $\boldsymbol{Q}(\sqrt{-1})$ and $\boldsymbol{Q}(\sqrt{-3})$, we have $a \pm b \pm c = 0$. Assume that F contains Eisenstein field $\boldsymbol{Q}(\sqrt{-3})$. Thus $\ell = -3$. Then for the case (i) or (iii), $\boldsymbol{Q}(\sqrt{mn\ell})$ is imaginary. Then by (5), we have $2d \pm 1 \pm 1 = 0$. This does not occur because $d \geq 2$. In the case (ii), by (2) we have $3 \pm 1 \pm 2m = 0$ for an odd $m > 0$, hence $m = 1$. By (7), we get $1 \pm 1 \pm 2n = 0$ and $n < 0$, hence $n = -1$. By (1), we have $-3 \pm 2d \pm 1 = 0$, hence $d = 2$. Thus $F = \boldsymbol{Q}\left(\sqrt{-1}, \sqrt{-2}, \sqrt{-3}\right)$. This field F coincides with the cyclotomic one $\boldsymbol{Q}(\zeta_{24})$ of conductor 24 and in fact $Z_F = \boldsymbol{Z}[\zeta_{24}]$.

Next let F be an imaginary field which does not contain Eisenstein field $\boldsymbol{Q}(\sqrt{-3})$. In the case (i) or (v), it holds that $1 \pm 1 \pm 2m = 0$ by (6) and $1 \pm 1 \pm 2n = 0$ by (7),

hence $m = n = \pm 1$, which contradicts to $mn \equiv 3 \pmod 4$. In the case (iii) or (iv), by (5) $2d \pm 1 \pm 1 = 0$ holds, which contradicts to $d \geq 2$.

For the case (ii), by (7) $1 \pm 1 \pm 2n = 0$, hence $n = -1$ holds and $\boldsymbol{Q}(\sqrt{dm})$ for (3) is a real field. On the rank r_3 of the matrix attached to the equation (3), if $r_3 = 1$, then by Lemma 4.2, $\ell \pm 1 \pm 2n = 0$, hence $\ell = -3$, which contradicts to the assumption. Then $r_3 = 2$. In the sequel, Proposition 4.6 is available for the quadratic fields of even discriminant corresponding to the cases (3), (5), (6), (7). By the equation (3) in $\boldsymbol{Q}(\sqrt{dm})$ we have

$$\frac{\ell}{\pm U_s} = \frac{1}{-U_{-t}} = \frac{-2}{U_{-u}} = 1 \quad \text{with} \quad s - t - u = 0,\ s, t, u > 0.$$

Then $U_u = 2U_t$. So $U_u \geq U_{t+1} = U_t T_1 + U_1 T_t \geq 2U_t = U_u$. Thus we have $s = 3, t = 1, u = 2, T_1 = U_1 = 1$. Namely, by $T_1^2 - dmU_1^2 = \pm 1, dm = 2$, i.e., the fundamental unit ε in $\boldsymbol{Q}(\sqrt{2})$ is $1 + \sqrt{2}$. Then we have the Pell sequence $\{U_s\} = \{1, 2, 5, \cdots\}$ with the recursive formula $U_{s+2} = 2U_{s+1} + U_s$ for any index s. Then we have $\ell = -U_3 = -5$ since $\ell < 0$. But this does not occur, because $\ell \equiv 1 \pmod 4$. Therefore we obtain $F = \boldsymbol{Q}(\zeta_{24})$ only, if F is imaginary.

Finally, we consider the case that F is real. On the rank r_7 of the equation (7), if $r_7 = 1$, then we have $1 \pm 1 \pm 2n = 0,\ n = 1$. Further on the rank r_3 of the equation (3), if $r_3 = 1$, we have $\ell \pm 1 \pm 2 = 0$, hence $\ell = 3$, which contradicts to $\ell \equiv 1 \pmod 4$. Then $r_3 = 2$. Thus in the same way as above, we have $dm = 2$, hence $m = n = 1$, which contradicts to $mn \equiv 3 \pmod 4$. Therefore $r_7 = 2$. Similarly, on the rank r_6 of the equation (6), we have $r_6 = 2$. Further on the rank r_5 of the equation (5), $r_5 = 2$, otherwise $2d \pm 1 \pm 1 = 0$, which contradicts to $d \geq 2$. By (7), since $r_7 = 2$, we have

$$\frac{1}{-U_{-s}} = \frac{1}{-U_{-t}} = \frac{2n}{U_u} = 1 \quad \text{with} \quad -s - t + u = 0,\ s, t, u > 0.$$

Then $s = t, u = 2s$. By Lemma 4.2, we may put $s = t = 1, u = 2$ and $U_1 = 1$, $U_2 = 2T_1U_1 = 2n$, hence $T_1 = n$ in $\boldsymbol{Q}(\sqrt{dm\ell})$. Similarly we obtain $T_1' = m$ in $\boldsymbol{Q}(\sqrt{dn\ell})$ by (6) and $T_1'' = d$ in $\boldsymbol{Q}(\sqrt{mn\ell})$ by (5). Since the field discriminants of the above three quadratic subfields of F are even, we have for integers $U^{(j)}$

$$n^2 - dm\ell U^2 = \pm 1, \quad m^2 - dn\ell U'^2 = \pm 1, \quad d^2 - mn\ell U''^2 = \pm 1.$$

Thus it follows that;

$$\begin{aligned}(dmn)^2 &= (dm\ell U^2 \pm 1)(dn\ell U'^2 \pm 1)(mn\ell U''^2 \pm 1)\\ &\geq (dm\ell - 1)(dn\ell - 1)(mn\ell - 1)\\ &> (dm)(dn)(mn)\\ &= (dmn)^2.\end{aligned}$$

This is a contradiction. Then if F is real, F is non-monogenic. Therefore we have completely proved Theorem. ∎

In general, for the case of $d_1m_1n_1 \neq 1$, we propose the following:

Problem. *Let $F/\boldsymbol{Q}$ be an octic Galois extension whose Galois group is 2-elementary abelian. Then, if F is monogenic, does F coincide with the field $\boldsymbol{Q}(\zeta_{24})$?*

References

[CF] J. W. S. Cassels and A. Frőhlich, Algebaic number theory, Academic Press, London and New York, 1967.

[DK] D. S. Dummit and H. Kisilevsky, *Indices in cyclic cubic fields*, in "Number Theory and Algebra." pp29-42, Collection of Papers Dedicated to H. B. Mann. A. E. Ross and O. Taussky-Todd, Academic Press, New York/San Francisco/London, 1977.

[F] G. Fujisaki, Algebraic number theory II (in Japanese), Shokabo 1975, 123-132.

[Ga_1] I. Gaál, *Computing all power integral bases in orders of totally real cyclic sextic number fields*, Math. Comp. **65**(1996), 801-822.

[Ga_2] I. Gaál, Diophantine Equations and Power Integral Bases, New Computational Methods, 2002, Boston·Basel·Berlin, Birkhäuser.

[GPP] I. Gaál, A. Pethő and M. Pohst, *On the Resolution of Index Form Equations in Biquadratic Number Fields* III. *The Bicyclic Biquadratic Case,* J. Number Theory, **55** (1995), 104-114.

[Gr_1] M.-N. Gras, *Non monogénéité de l'anneau des entiers de certaines extensions abéliennes de* $\boldsymbol{Q}$, Publ. Math. Fac. Sci. Besançon, Theor. Nombres 1983-1984. Exp. No. 5 (1984), 25pp. degré premier $\ell \geq 5$,

[Gr_2] M.-N. Gras, *Non monogénéité de l'anneau des entiers des degré premier* $\ell \geq 5$, J. Number Theory, **23** (1986), 347-353.

[GT] M.-N. Gras and F. Tanoé, *Corps biquadratiques monogènes,* Manuscripta Math., **86**(1995), 63-77.

[Gy_1] K. Győry, *Sur les polynômes á coefficients entiés et de discriminant donné V*, Acta. Math. Sci. Hungry, **32** (1978), 175-190.

[Gy_2] K. Győry, *Discriminant form and index form equations*, in "Algebraic Number Theory and Diophantine Analysis" (F. Halter-Koch and R, F. Tichy. Eds.) pp. 191-214, Walter de Grunter, Berlin New York, 2000.

[HK] F. Halter-Koch, *Geschlechtertheorié der Ringklassenkőrper,* J. Reine Angew. Math., **250**(1971), 107-108.

[HSW] J. G. Huard, B. K. Spearman and K.S. Williams, *Integral bases for quartic fields with quadratic subfields*, J. Number Theory **51** (1995), 87-102.

[Ko] B. Kovács, *Canonical number systems in algebraic number fields*, Acta. Math. Acad. Sci. Hungar. **37**(1981), 159-164.

[KP] B. Kovács and A. Pethő, *Number Systems in Integral Domains, Especially in Orders of Algebraic Number Fields*, Acta. Sci. Math. **55**(1991), 287-299.

[Ku] T. Kubota, Lectures on Number Theory — Metaplectic Theory and Geometric Reciprocity Law — (in Japanese), Makino-Shotenn, Tokyo,1999, p. 228.

[La] S. Lang, "Algebraic Number Theory." Addison-Wesley Publishing Company, Inc., Reading, MA. 1970.

[Le] H.-W. Leopoldt, *Über die Hauptordnung der ganzen Elemente eines abelschen Zahlkörpers*, J. Reine Angew. Math. **21**(1959), 119-149.

[M_1] Y. Motoda, *On Biquadratic Fields*, Mem. Fac. Sci. Kyushu Univ., Series A, **29**-2 (1975), 263-268.

[M_2] Y. Motoda, *Notes on Quartic Fields*, Rep. Fac. Sci. Engrg. Saga Univ. Math. **32**-1 (2003), 1-19.

[M_3] Y. Motoda, *On Integral Bases of Certain Real Monogenic Biquadratic Fields*, Rep. Fac. Sci. Engrg. Saga Univ. Math. **33**-1 (2004), 9-22.

[MN_1] Y. Motoda and T. Nakahara, *Monogenesis of Algebraic Number Fields whose Galois Group are* 2*-elementary Abelian*, Proceedings of the 2003 Nagoya Conference "Yokoi-Chowla Conjecture and Related Problems", Furukawa Total Printing Co., 2004, 90-99.

[MN_2] Y. Motoda and T. Nakahara, *Power Integral Bases in Algebraic Number Fields whose Galois Group are* 2*-elementary Abelian*, Arch. Math., in press.

[MNS] Y. Motoda, T. Nakahara and S. I. A. Shah, *On a Problem of Hasse for Certain Imaginary Abelian Fields*, J. Number Theory **96** (2002), 326-334.

[Nak_1] T. Nakahara, *On Cyclic Biquadratic Fields Related to a Problem of Hasse*, Mh. Math. **94**(1982), 125-132.

[Nak_2] T. Nakahara, *On the Indices and Integral Bases of Non-cyclic but Abelian Biquadratic Fields*, Arch. Math. **41** (1983), 504-508.

[Nak_3] T. Nakahara, *On the Indices and Integral Bases of Abelian Biquadratic Fields*, RIMS Kōkyūroku, Distribution of values of arithmetic functions, **517** (1984), 91-100.

[Nak_4] T. Nakahara, *On the Minimum Index of a Cyclic Quartic Field*, Arch. Math. **48**(1987), 322-325.

[Nak_5] T. Nakahara, *A simple proof for non-monogenesis of the rings of integers in some cyclic fields*, in "Advances in Number Theory", ed. by F. Q. Gouvéa and N. Yui, Clarendon Press, Oxford, 1993, 167-173.

[Nar] W. Narkiewich, Elementary and analytic Theorey of Algebraic Numbers, 2nd Edition, 1990, Springer-Verlag, Berlin Heidelberg New York; Warszawa, PWM-Polish Scientific Publishers.

[Ok] S. Oka, *On the unramified common divisor of discriminants of integers in a normal extension*,Nagoya Math. J. **160** (2000), 181-186.

[Ol] P. Olajos, *Power Integral Bases in a Parametric Family of Sextic Fields*, Publ. Math. Debrecen. **58** (2001), 779-790.

[Pe] A. Pethő, *Connections between power integral bases and radix representations in algebraic number fields*, preprint.

[Ri] P. Ribenboim, The Fibonacci numbers and the Arctic Ocean, Proceedings of the 2nd Gauss Symposium. Conference A: Mathematics and Theoretical Physics (Munich, 1993), 41-83, Sympos. Gaussiana, de Gyuyter, Berlin, 1995.

[Ro_1] L. Robertson, *Power Bases for Cyclotomic Integer Rings*, J. Number Theory **69** (2001), 98-118.

[Ro_2] L. Robertson, *Power Bases for* 2*-power Cyclotomic Fields*, J. Number Theory **88** (2001), 196-209.

[Sc] R. Schertz, *Konstruktion von Potenzganzheitsbasen in Strahlklassenkörpern über imaginär-quadraticshen Zahlköpern*, J. Reine Angew. Math. **398**(1989), 105-129.

[Sh] S. I. A. Shah, *Monogenesis of the Ring of Integers in a Cyclic Sextic Field of a Prime Conductor*, Rep. Fac. Sci. Eng. Saga Univ. Math. **29**-1 (2000), 1-10.

[SN_1] S. I. A. Shah and T. Nakahara, *Non-monogenetic Aspect of the Ring of Integers in Certain Abelian Field*, Proceedings of the Jangjeon Mathematical Society, **1**(2000), 75-79.

[SN_2] S. I. A. Shah and T. Nakahara, *Monogenesis of the Rings of Integers in Certain Imaginary Abelian Fields*, Nagoya Math. J. **168** (2002), 85-92.

[ST] J. H. Silverman and J. Tate, *Rational Points in Elliptic Curves*, Undergraduate Texts in Mathematics, Springer-Verlag, 1992.

[Tak] T. Takagi, Algebraic number theory (in Japanese), Iwanami 1971.

[Tan] F. Tanoé, Monogénéité des corps biquadratiques, L'Université de Franche-Comté, 1990 (Thèse).

[Th] J.-D. Thérond, *Existence d'une extension cyclique monogéne de discriminant donné*, Arch. Math. **41**(1983), 243-255.

[Uc] K. Uchida, *When is* $\boldsymbol{Z}[\alpha]$ *the ring of integers?*, Osaka J. Math. **14**(1977), 155-157.

[Wa] L. C. Washington, Introduction to cyclotomic fields, Graduate texts in mathematics **83**, Springer-Verlag, New York Heidelberg Berlin, 1980.

[Wi] K. S. Williams, *Integer of biquadratic fields*, Canad. Math. Bull. **13**-4 (1970), 519-526.

[Ży] E. von Żyliński, *Zur Theorie der außerwesentlichen Diskriminantenteiler algebraischer Körper*, Math. Ann. **73** (1913), 273-274.

Yasuo Motoda
Yatsushiro National College of Technology, 866-8501 Yatsushiro, Japan
e-mail: motoda@as.yatsushiro-nct.ac.jp